2004 Academy of International Business (AIB) Southeast Asia Regional Conference

Security Risk Management Issues in Maritime Trade: An Analysis.

by

Dr Paul Barnes,

School of International Business
Queensland University of Technology
GPO Box 2434, Brisbane, QLD 4001 Australia
Tel: +61 7 3964 9019; Fax: +61 7 3864 1771;
E-mail: p.barnes@qut.edu.au

Security Risk Management Issues in Maritime Trade: An Analysis.

Abstract:

Security is currently a key factor in the evolution of international trade, and maritime trade in particular, with a number of internationally mandated and voluntary initiatives underway focusing on vulnerabilities in supply and logistics chains. This paper suggests the combined effect of these initiatives, with suitable systems of risk management embedded in private and public sector groups within the industry may be more effective in mitigating the threat of maritime terrorism than with the initiatives alone. The paper then draws on approaches to risk and crisis management in complex systems to examine options for integrating in-country and international frameworks.

Keywords: Maritime Security, Risk Management, Vulnerability.

Introduction:

The events of September 11, 2001 precipitated a range of unilateral and multilateral responses to security threats internationally. While an obvious initial focus of crisis management in the United States (U.S.) was shutting down domestic air space, attention moved quickly to security in maritime transport and specifically to maritime trade as vector for the delivery of terrorist acts to the U.S. mainland. Particular emphasis was given to the global sea-container shipping system and vulnerabilities inherent within industry practice.

The International Maritime Organisation (IMO) and other groups such as the World Customs Organisation (WCO) have jointly supported processes to enhance regulatory coverage of safety and security within the world trading system. The IMO has promoted a number of security measures including changes to the Safety of Life at Sea (SOLAS) Convention addressing ship security with new requirements for an International Ship and Port Facility Security (ISPS) Code.

Inter alia to these changes the U.S. has proposed a series of voluntary programmes aimed at enhancing security of trade into North American seaports. While not binding on trading partners, the measures are intended to provide levels of security assurance and facilitate enhanced movement of cargo by participating ports, carriers and companies. These measures are intended to provide a competitive advantage to early voluntary adopters over time. The two principal American voluntary programmes are the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C-TPAT).

While the CSI and C-TPAT are sound strategies for addressing container security, there is recognition that these programs represent only a framework for building a maritime security regime, and that significant gaps in security coverage remain (Frittelli, 2003). Beyond the contention of ongoing gaps in security coverage there is, arguably, varied appreciation of the complexity of the international trading system itself, in particular the interface between port and host country.

This paper argues that the expected reliability and assurances of security in maritime trade will derive not merely from the adoption of mandated or voluntary security frameworks but as a result of implementing them by the organisations and businesses operating in, and

providing services to, ports and combining them with suitable systems of risk and crisis management.

After detailing a number of recognised risk factors within the international maritime system the paper examines aspects of the current security initiatives. Then drawing on findings from research into organisational responses to large-scale crises the paper discusses the need to ensure that maritime security regimes are appropriately embedded into the risk management systems used by organisations managing port-based infrastructure and interface with other international trade-related and security assurance systems operating with the port's host country.

Risk factors in Maritime Trade:

Concern about shipping as a terrorist vector by the U.S. (with growing recognition in many other countries) is easily understood when noting that in 2001, approximately 5.400 commercial ships (most not registered in the U.S. and crewed by non-US nationals) made near to 60,000 port visits (APEC, 2003a). Additional context is added by the recognised complexity of port operations and the difficulty in effectively implementing security coverage over them (Hecker, 2002 and Harrald *et. al.* 2004).

It has been estimated that up to 90% of world cargo movement occurs in shipping containers with up to 250 million movements each year. It is further estimated that a mere 2% of this volume is physically inspected post-arrival (Van de Voort *et. al.*, 2003; OECD, 2003b).

Concerns about security risk emerge from the interaction of a number of factors:

- *Cargo* - using cargo to smuggle people and/or weapons (of a conventional, nuclear, chemical or biological nature).
- *Vessel* - using the vessel as a weapon or means to launch an attack (including sinking a vessel to disrupt infrastructure)
- *People* - attacking the ship to cause human casualties (or using the cover of seafarer identities to insert terrorist operatives).
- *Money* - using revenue from shipping to fund terrorist activities or the launder money for terrorist organisations (OECD, 2003b).

Evidence that concerns such as these are credible is offered in the widely reported incident of a stowaway in a shipping container detailed below:

> In October 2001, authorities in the southern Italian port of Gioia Tauro discovered an unusually well-equipped and neatly dressed stowaway locked inside a shipping container. It was furnished as a makeshift home with a bed, water, supplies for a long journey and a bucket for a toilet. Italian police named the stowaway as Rizik Amid Farid, 43, and said he was born in Egypt but carried a Canadian passport. Unlike most stowaways, he was smartly dressed, clean-shaven and rested as he emerged.
>
> He was found to be carrying two mobile phones, a satellite phone, a laptop computer, several cameras, batteries and, ominously given recent events in the US, airport security passes and an airline mechanic's certificate valid for four major American airports. He was carrying a return airline ticket from Montreal, Canada, to Egypt via Rome. Italian investigators said that the air ticket could be an "insurance policy" enabling him to reach Canada by air in case he was discovered in the container but managed to escape after being released from custody on bail. OECD (2003 b)

Whether such incidents are frequent may not be easy to confirm but the detail of the discovery does validate the existence of a viable threat.

Fleet Ownership

A further factor of concern is transparency in ship registration and ownership. A recent study on the ownership and control of ships (OECD, 2003c) suggests that in addition to the absence of clarity on registration details, anonymity of ownership is a standard industry practice rather than the exception. The use of 'flags-convenience' mechanisms are legally tolerated in almost all national jurisdictions and might enable terrorists or criminal elements to operate or influence the use of vessels behind a cloak of anonymity.

False Documents

Identity and qualification fraud is also a concern. Sea faring jobs are relatively highly paid with the international benchmark for a deck hand in late 2003 of US$ 1,300 per month (Richards (2004a). Richards (2004a) further reports that with demand outstripping supply and with regulation and recruitment and manning practices is lax, fraud and corruption is prevalent.

Evidence has shown that a large number of qualification certificates held by seafarers are fraudulent and that fake papers for crew members can be bought and sold easily. In 2001 the Seafarers International Research Centre (SIRC) reported on a survey of 97 maritime

administrations on the prevalence of certification fraud. Of the 54 respondents, 82% had discovered this type fraud within its constituency.

In a further example of this problem, the International Transport Workers' Federation (ITF) bought a First Officer's certificate for its General Secretary. The certificate and seaman's book (costing $US4,500), authorised him to navigate a vessel and deputise for its captain despite his complete lack of marine qualifications and skills. The ITF says that fake certificates have remained a problem as late as mid-2003 (Richards, 2004a).

Piracy

The sea is a domain that can barely be policed although there is a critical need to enforce relevant law and international treaties. This especial important given continued existence of modern and sophisticated strains of piracy and its politicised cousin, the maritime form of the new stateless terrorism (Langewiesche, 2003). Piracy is a well noted security issue internationally with known geographical areas of concern in the south East Asian region (Richardson, 2004a & 2004b; Anonymous, 2004; Jarvis, 2003; OECD, 2003b). The IMO has reported a total of 45 instances of piracy (forced boarding, cargo hi-jacking and violent assault on crews) in their reporting category the 'Far East,' in the second quarter to June 2003 (Jarvis, 2003). Over the ten year period 1993 to 2003 a total of 3,254 acts of piracy have been recorded in this geographical category.

Ports as Critical Infrastructure

In recent times ports have become pieces of critical infrastructure within the trading system. Certain locations classify as "hub Ports" that due to their size and capacity have become essential to the global supply chain (Bateman, 2003). Recent post September 11 concerns about maritime commerce relate to the impact of a terrorist incident in such a location and the disruptive effect on seaborne trade. Ships can usually re-route around a chokepoint, at cost in terms of time, but loss of a substantial facility is a major critical infrastructure protection issue. A further element requiring protection at a port is the automated control systems used including, in particular, embedded information technology and information systems.

Insurance

A sea-borne terrorist incident whether using conventional or improvised explosive devices or involving chemical, biological or nuclear materials would impact heavily on the availability and cost of marine insurance. Premiums were tripled for ships calling at ports in Yemen after the 2002 terrorist attack on French oil tanker Limburg off the Yemeni coast. This forced many vessels to cut Yemen from their schedules or divert to ports in neighbouring states. In addition to increased insurance and re-insurance costs a catastrophic sea-borne terrorist attack would cause delays in shipping or in a best case, increase transit times for commodity movements. Such disruptions of the supply chain would have repercussions around the world and profoundly affect business confidence (Richardson, 2004b)

Current Maritime Security Measures

The ongoing maintenance of trade and transport efficiency is an ideal outcome from any maritime security regime. The new maritime security measures have emerged from two fora: mandated requirements from the IMO in the form of the ISPS Code. Two voluntary initiatives are being promoted by the U.S in response to its own security analysis of the vulnerabilities of the maritime transport system - the CSI and the C-TPAT (OECD, 2003b). Each of these initiatives is discussed below.

International Ship and Port Facility Security (ISPS) Code

The requirements defined in the ISPS Code can be broadly broken down into a number of major categories according to their focus. These are listed in Table 1 along with estimated establishment and yearly maintenance costs.

Table 1: ISPS Code Requirements against Maritime Industry Sectors (OECD, 2003b).

Governments
• Determining which port facilities are required to designate a Port Facility Security Officer. • Ensuring completion and approval of a Port Facility Security Assessment and the Port Facility Security Plan for each port facility that serves ships engaged on international voyages. • Approving Ship Security Plans and amendments to previously approved plans. • Verifying compliance of ships and issuing the International Ship Security Certificate, and any subsequent amendments; and exercising control and compliance measures. − Communicating information to the International Maritime Organization and to the shipping and port industries

Table 1: Contd.

Maritime carrier companies Initial Cost (million USD) **$1170.6** Yearly Costs (million USD) **$725.6**
Companies will: • Designate a Company Security Officer (CSO). • Undertake a Ship Security Assessment (SSA), including an on-site visit, for every vessel to be issued a SSC. • Develop a Flag-State-approved Ship Security Plan (SSP) that references the individual ship's SSA and incorporates all of the elements included in part "A" of the ISPS Code. • Designate a Ship Security Officer (SSO). • Provide adequate training for the CSO, SSO and crew and ensuring that adequate drills and exercises are carried out. • Ensure that vessels are equipped to carry out the security procedures outlined in their SSP's. • Ensure adequate security-related record-keeping.

Table 1: Contd.

Ships (requirements) Initial Cost (million USD) **$757.4** Yearly Costs (million USD) **$4.3**	
Automatic Identification System	Ship-borne communication devices detailing to other AIS transponders and shore-based facilities information on the ship's identity, position, heading and speed (Primarily designed to enhance the safety of navigation in crowded areas).
Identification number	Vessels must have a unique identification number. This number must be displayed by July 1, 2004.
Security alert system	All passenger ships, high-speed cargo vessels, chemical tankers, oil tankers and gas carriers of more than 500 gross tons must be fitted with a Ship Security Alert System that will: • Initiate and transmit a ship-to-shore security alert to a competent authority designated by the Flag administration**,** which in these circumstances may include the company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised. • Not send the ship security alert to any other ships. • Not raise any alarm on-board the ship. • Continue the ship security alert until deactivated and/or reset. • Be capable of being activated from the navigation bridge and in at least one other location. • Conform to performance standards not inferior to those adopted by the IMO.

Table 1: Contd.

Ports	
Initial Cost (million USD) **$55.8**	Yearly Costs (million USD) **$1.6**
Port facilities that receive vessels engaged in international trade will be required to: • Carry out, and have approved, port facility security assessments. • Develop port facility security plans that detail measures to be taken at each security alert level, and address single-ship security alerts. • Designate a Port Facility Security Officer (PFSO) with skills and training roughly similar to the CSO. • Ensure that the PFSO and other appropriate personnel receive adequate training to carry out their duties and that security drills are held to ensure the readiness. • Ensure that port facilities are sufficiently equipped and staffed in order to operate under relevant security levels • Certification/documentary requirements.	

The detailed requirements of the ISPS code address a number of the risk factors listed earlier. Ship identification, security planning and alert systems have been mandated as well as detailed requirements for maritime carriers. On obvious emphasis is on ship owners and ensuring that ships have the capacity to report alerts while underway. The initial outlay for the ISPS is estimated to cost $1,983.8 million USD with an annual maintenance cost of $731 million.

Container Security Initiative (CSI)

The CSI seeks to develop bi-lateral agreements between the United States and foreign countries to pre-screen high-risk containers in ports of loading. While the majority of containers do not pose any security threat all identified high-risk containers will be inspected, either before loading at a CSI port or, if arriving from another port, upon arrival in the United States. In CSI ports, local customs officials and U.S. Bureau of Customs and Border Protection staff would jointly decide on which containers to inspect before loading. The initiative is built around 4 principal elements shown Table 2 below.

Table 2: Elements of the CSI (OECD, 2003b).

• Establish security criteria to identify high-risk containers. • Pre-screen those containers prior to American arrival (Involves the deployment of American Customs officials to foreign ports). • Use technological means to pre-screen these containers. • Develop and use IT-enabled and secure containers.

The C-TPAT is the second major voluntary security initiative promoted by the U.S. The C-TPAT aims to ensure that participants implement policies, plans and procedures to ensure the integrity of their entire supply chain. Participants will be expected to sign agreements committing to the following four actions listed in Table 3.

Table 3: Requirements for C-TPAT (OECD, 2003b).

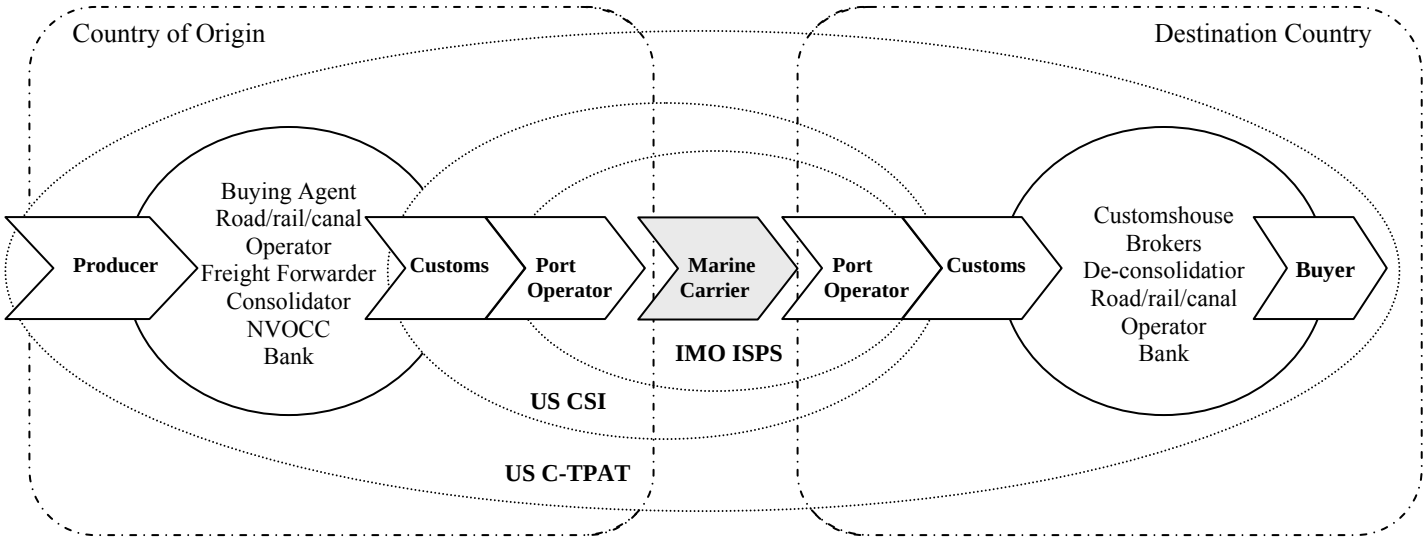
Participants are expected to:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by U.S. Customs and the trade community. The guidelines encompass: Procedural Security, Physical Security, Personnel Security, Education and Training, Access Controls, Manifest Procedures, and Conveyance Security (Participants must also submit a supply chain security profile questionnaire to U.S. Customs).
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

In return for agreement to and implementation of these additional initiative and the validation of the participant's plans, it has been suggested that C-TPAT participants are less likely to be targeted for customs inspections and would benefit from expedited customs procedures in the medium short to medium term.

The scope of all three maritime security initiatives is shown in Figure 1. The ISPS code focuses on maritime carriers and ships with particular legislative roles for national governments. The CSI seeks to expedite the identification of higher risk containers and pre-screen them before allowing on-forwarding to intended destinations.

Figure 1: Scope of IMO and US Maritime Security Initiatives
(OECD 2003c)



C-TPAT framework attempts to overlay an extensive screening and assessment regime across supply chains to include both infrastructure and functionaries in a country-of-origin and those in the country-of-destination.

The costs of complying with both the CSI and C-TPAT initiatives is undetermined and would vary depending on pre-existing risk management systems in place at major ports. Beyond issues of costs it is likely that full implementation of the C-TPAT system, because of its intrusive scope, would require detailed negotiations among companies and authorities engaged in international trade in all trading countries.

The potential costs to participants are great as they must invest in securing the physical integrity of their own premises and that of their trading partners as well. Other costs include training staff, adding security guards, developing security risk management plans and processing C-TPAT paperwork. It is likely that involvement in the C-TPAT initiative will require substantial investment for many industry sectors however many already have effective security practices in place to reduce the theft. The latter will likely face lower participation costs (OECD, 2003b).

Regional Diplomacy

Acceptance of the intrusiveness of the C-TPAT initiative is likely to require considerable negotiation with many countries. Within our local area an ongoing process of national consultation and cooperation on preventing terrorism, including maritime piracy is being promoted under auspices of the Asia Pacific Economic Cooperation (APEC) and the Association of South East Asian Nations (ASEAN) (APEC, 2003a). .

The Secure Trade in the APEC Region (STAR) Initiative for example seeks to strengthen maritime security against terrorism while boosting trade efficiency. In addition to supporting the implementation of the ISPS Code, this initiative encourages implementation of common standards for electronic customs reporting (a World Customs Organisation program), support baggage screening procedures and mandatory aviation security audits (required by the International Civil Aviation Organisation), and for implementation of a common standard for the collection and transmission of advanced passenger information to prevent the fraudulent use of travel documents by terrorists APEC (2003a).

The STAR Initiative seeks to generate new partnerships between government and business at the national and international level resulting in mitigation of terrorist or criminal threats throughout the supply and logistics chain.

Members of ASEAN are encouraging a shift in the focus of the ASEAN Regional Forum (ARF) from traditional attention to inter-state power relations towards commonly perceived threats such as international terrorism, piracy at sea, arms smuggling and other trans-national crimes. Greater cooperation has been pledged by ARF members on these areas of concern, in particular, threats to maritime security (Severin, 2003). Dialogue on these broader issues including trans-national crime is also to be progressed through the activities of the Council for Security Cooperation ion Asia Pacific (CSCAP, 2003).

This expanding dialogue is needed urgently if ASEAN is serious in achieving a European Union-like economic community by the year 2020, as recently reported (Hew, 2003). The resurgence of border and trade security as an issue in Europe, recently, has firmly established regional cooperation on a range of security issues as a critical factor (European Commission, 2004). While the interactive complexity among 25 land-locked European nations is obviously great the requirements of trade across land and maritime borders, as in South-East Asia, seem more challenging by orders of magnitude.

Managing Risk in Complex Systems

The maritime supply chain is susceptible to the effects of terrorism and other varieties of perturbation because of its global and open nature, and its complexity (Van de Voort, M., *et. al.*, 2003). Further, the complex organisation and unique vulnerabilities of ports and associated support components are not easily appreciated or understood (Harrald, Stephens & van Dorp, 2004). The U.S. Government Accounting Office has suggested also that difficulties in coordination among public and private entities with an interest in port security, generally, may make effective security programs hard to establish (Hecker, 2002).

A security incident (or a multiple concurrence of incidents) could occur at any time along a supply chain network. By design and function the current maritime trade initiatives discussed in this paper (other than ship-specific practices) are more suited to reducing the

likelihood of incidents rather than to respond to or resolve them. The capacity to respond to incidents, whether at a port or at sea, will be dependent on the security infrastructure and emergency systems in-place locally and maritime resources available. The effectiveness of the C-TPAT initiative, in particular, will also be dependent on local systems and the interactive efficiencies of these systems.

Accidents in large highly complex systems can occur in a number of ways. They may emerge suddenly due to the interaction of previously separated system elements or may cook slowly (without recognition) until they appear. In either case the accidents (incidents) are often surprising and unexpected. There is a well established literature on complex systems failures where, on investigation, evidence was discovered that there had been 'signs' that disaster was emerging from organisational 'noise' (Perrow, 1984; Turner & Pidgeon 1997; Boin & Lagadec, 2000; Comfort *et. al.*, 2001, Rijpma, 1997).

Organisations that fail to note the presence of 'warning signs' during the so-called 'incubation' of these failures have been termed 'crisis prone' (Mitroff *et. al.*, 1989; Pearson & Mitroff, 1993; Mitroff & Alpaslan, 2003). Crisis prone organisations may be more at-risk because of in-attentiveness to internal processes as well as the wider environment that they operate within.

Dysfunctional internal control and coordination mechanisms within a broader risk management/corporate governance framework may have resulted in a reduced capacity to detect warning signs or understand their meaning. Inflexible cultural factors or belief systems within an organisation itself might also contribute to this reduced awareness. Notions of in-vulnerability or indifference to external or internal threats (Boin & Lagadec, 2000) are examples of organisation-level issues.

Equally there are situations where, as a result of extreme systems complexity, warning signs might have been visible, or if detectable, not understood. While not the same category as the situation above, where a crisis signalling its arrival could have been detected, this second category could be the result of totally new systems behaviour or an incomplete understanding or appreciation of the system in question. The international maritime trading system, as a 'system of systems,' is a likely example of this.

Realistically a systems complexity continuum exists involving the port system and the wider trading system. Port management (and by default governments) have to deal with two forms of vulnerability within this continuum: *Internal* (a port-based system with sub-components, and related management structures); and *External* (the international trade system).

Although individual port elements (as stand alone sub-systems) may be tightly connected, the functional links to other systems within a port can be relatively loose. A container facility is for example, 'tightly coupled' with the inter-modal rail yard and the scheduled arrival of container vessels, but only loosely connected with the adjacent petroleum facility or cruise terminal. Similarly, cargo and passengers are transferred to and from the maritime mode connecting them with other transportation modes (e.g. rail, road, or pipeline) (Harrald, Stephens and van Dorp, 2004).

As noted above, processes at ports and in related systems, can be difficult to coordinate. The lack of awareness of a security incident in one sub-component may severely impact another. Other than provisions against criminal theft and violence, security may not have been a design criterion for any of these maritime sub-systems. This absence of in-built security in the segregated sub-systems may mean retro-fitting security at international ports will be more than just enhanced asset protection. A port security framework, logically, would need to extend well ashore within both the U.S. and international settings (e.g. security for container and other general trade movements) as well as at sea (passenger vessel). Currently, vulnerabilities inherent in such complex systems (ports) are not adequately understood (Harrald, Stephens and van Dorp, 2004).

The importance of ensuring that international ports and in-country essential services are fully integrated with on-site security systems is critical. Similarly, the CSI and C-TPAT initiatives will need a similar integration to maximise effectiveness. A third requirement is that organisations at a port must be crisis prepared and not crisis prone. Given the well established causal and contributory factors from the management of organisations during crises, this third requirement may be the most critical factor in a successful security regime for world trade.

Discussion

The C-TPAT and CSI frameworks are designed to focus on specific factors of supply chains and connect port operators to other port operators. As guidelines they are gently coercive to individual firms or providers of services within ports and indirectly, regional governments. While focused on key components of the supply chain they may also require attention to functions and activities that are additional to a firm's normal management practices and operational capabilities.

This paper argues that security initiatives alone will not provide assurance that the trading system is protected adequately and that an effective level of involvement by national port authorities, operators and regional governments is also required. In addition, there are a range capabilities and capacities both implicit and explicit in the ISP, CSI and the C-PTAT initiatives that may have to be developed within resident organisations.

One of these organisational level capabilities is Crisis Management. As mentioned earlier both 'slow' and 'rapid' onset crises emerge readily in highly complex systems. The degree of fore-warning is dependent often on the sophistication of existing organisational monitoring systems available. It is recognised that organisational performance declines during crises where conditions of increasing complexity, multiple levels of activity and increased flows of information impact adversely on human decision makers (Comfort *et. al.* 2001).

As mentioned earlier the presence of both internal and external vulnerability within systems increase the vigilance needed within organisations. Crises create situations that cannot be anticipated so 'warning sign' detection is critical as is a tested ability to respond to emergencies quickly and effectively (Boin & Lagadec, 2000).

A robust crisis management capability and capacity includes capabilities for:

- Environmental Scanning (Detection of weak signals)
- Emergency Management Escalation Triggers (incident or issue recognition) leading to rapid consequence analyses (in the context of high uncertainty)
- Crisis Management Decision-making Capacity (separate to routine business decision making structures)
- Clearly stated, understood and tested communication mechanisms for reporting emergent incident/issues to the port CEO and senior management of associated infrastructure and service providers (Barnes, 2001).

These crisis management capabilities match many of the known organisational factors that contribute to complex systems failures. The widespread prevalence of these capacities would enhance implementation of the ISPS, CSI and C-TPAT initiatives by providing the means for compliance with the guidelines. Confidence across regional boundaries that trading partners have similar and supportive detection and response capabilities would add to assurance on security.

Conclusion

Collectively the three security initiatives discussed here can provide dual-benefits to port operators and onsite businesses that extend beyond just reducing the likelihood of terrorist acts perpetrated through the maritime trading system.

An effective security regime within maritime trade, however, will require more than just the implementation of these systems but the recognition and response to organisational complexity at two levels: (1) at Ports and port-related infrastructure and (2) within the interconnected 'system of systems' that is the world maritime trading network.

Achievement of a measure of influence over both internal and external vulnerability will require an enhanced awareness of how to design and operate management systems that are both flexible and self-regulatory, exhibiting attention to detail and able to accommodate uncertainty and the unexpected.

References:

Anonymous (2004) *The Rising East: Pirates and Terrorism*, Editorial, [www document] http://www.koreaherald.co.kr/SITE/data/htnl dir/2004/03/05/20403050015.

APEC (2003) *Strengthening International Cooperation and Technical Assistance in Preventing and Combating Terrorism*, Intervention by APEC Secretariat at the 12th Session of the Commission on Crime Prevention and Criminal Justice, 16-19 May, Vienna, Austria.

Barnes, P (2001) *Crisis Management Needs in the Public Sector*, State Conference, Institute of Public Administration Australia Queensland Division, 24 August.

Bateman, S. (2003) 'Maritime Security: A New Environment Following September 11,' in the Symposium of Maritime Experts to Assist in Implementation of the STAR Initiative, Melbourne, 18 – 20 June.

Boin, A. and Lagadec, P. (2000) 'Preparing for the Future: Critical Challenges in Crisis Management,' *Journal of Contingencies and Crisis Management*, 8(4): 185-191.

Comfort, L. et. al. (2001) 'Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments,' *Journal of Contingencies and Crisis Management*, 9(3): 144-157.

CSCAP (2003) 'Report of the general Conference of the Council for Security Cooperation in the Asia Pacific,' CSCAP, Jakarta, December 7-9.

European Commission (2004) *Research for a Secure Europe: Report of the Group of Personalities in the field of Security Research*, European Commission, [www document] http://europa.eu.int/comm/research/security/

Frittelli, J. F. (2003) *Port and Maritime Security: Background and Issues for Congress*, Congressional Research Service, December 5.

Harrald, J. R., Stephens, H. W. and van Dorp, J. R. (2004) 'A Framework for Sustainable Port Security,' *Journal of Homeland security and Emergency Management*, 1(2):1-13.

Hecker, J. Z. (2002) *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, U.S. General Accounting Office, August 1.

Hew, D. (2003) 'Towards an ASEAN Economic Community by 2020: Vision or Reality?,' *Viewpoint* - Institute of South east Asian Studies, [www document] www.iseas.edu.sg/viewpoint.

Jarvis, D. S. L. (2003) The Arc of Instability: Regional Security Challenges for Australia and the Asia Pacific, Centre for International Risk, The University of Sydney.

Langewiesche, W. (2003) **'**Anarchy at sea,' *The Atlantic Monthly***,** Sep., 292 (2): 50-70

Mitroff, I.I. & Alpaslan, M.C. (2003) 'Preparing for Evil,' *Harvard Business review*, April: 109 -115.

OECD (2003a) 'Lessons Learned in Dealing with Large-scale Disasters'," SG/AU(2003)1.

OECD (2003b) *Security in Maritime Transport: Risk factors and Economic Impact*, Maritime Transport Committee, Directorate for Science, Technology and Industry, July.

OECD (2003c) *Ownership and Control of Ships,* Maritime Transport Committee, Directorate for Science, Technology and Industry, March.

Pearson, C.M. and Mitroff, I.I. (1993) 'From Crisis Prone to Crisis Prepared: Framework for Crisis Management,' Academy of Management Executive, 7(1): 48-106.

Perrow, C. (1984) *Normal Accidents: Living with High Risk Technologies*, Basic Books, New York.

Richardson, M. (2004a) 'A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction,' *Viewpoint* - Institute of South east Asian Studies, [www document] www.iseas.edu.sg/viewpoint.

Richardson, M. (2004b) 'Growing Vulnerability of Seaports from Terror Attacks, to protect ports while allowing global flow of trade is a new challenge,' *Viewpoint* - Institute of South east Asian Studies, [www document] www.iseas.edu.sg/viewpoint.

Rijpma, J.A. (1997) Complexity, Tight-coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory, *Journal of Contingencies and Crisis Management*, (5)1:15-23.

Severin, R. C. (2003) 'ASEAN: Security and Development Challenges,' Asian Institute of Management, at the 6th Lecture Series of the Ramos Peace and Development Foundation, Makati, 29 August, [www document], www.iseas.edu.sg/viewpoint/mr5mar04.pdf

Turner, B.A. and Pidgeon, N. (1997) *Man-made Disasters (2nd Edn*), Butter-worth Heineman, Oxford.

Van de Voort, M., *et. al.* (2003) *Seacurity (Improving The Security of the Global Sea-Container Shipping System)*, RAND Europe, MR-1695-JRC.

Watkins, M.D. & Bazerman, M. H. (2003) "Predictable Surprises: The Disasters You Should Have Seen Coming," in the *Harvard Business Review*, March, pp. 72-80.

Watkins, M.D. & Bazerman, M. H. (2003) "Predictable Surprises: The disasters you should have seen coming," in The Harvard Business review, March, pp. 72-80.